UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,231	06/12/2001	Ron Karim	15437-0508	5058

45657 7590 02/27/2007

HICKMAN PALERMO TRUONG & BECKER, LLP
AND SUN MICROSYSTEMS, INC.
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110-1089

EXAMINER	
WU, QING YUAN	
ART UNIT	**PAPER NUMBER**
2194	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/880,231	KARIM, RON	
	Examiner	Art Unit	
	Qing-Yuan Wu	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-17 and 19-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-17 and 19-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-17 and 19-32 are pending in this application.

Response to Amendment

2. The amendment to the claims filed on 12/4/06 does not comply with the requirements of 37 CFR 1.121(c) because claims 3 and 19 were previously canceled. Reinstatement of the canceled claims should be presented as "new." Please see guideline below. For examination purposes these claims will be treated as newly added claims, however applicant should consider presented them as new claims in the next amendment.

3. Amendments to the claims filed on or after July 30, 2003 must comply with 37 CFR 1.121(c) which states:

(c) *Claims*. Amendments to a claim must be made by rewriting the entire claim with all changes (*e.g.*, additions and deletions) as indicated in this subsection, except when the claim is being canceled. Each amendment document that includes a change to an existing claim, cancellation of an existing claim or addition of a new claim, must include a complete listing of all claims ever presented, including the text of all pending and withdrawn claims, in the application. The claim listing, including the text of the claims, in the amendment document will serve to replace all prior versions of the claims, in the application. In the claim listing, the status of every claim must be indicated after its claim number by using one of the following identifiers in a parenthetical expression: (Original), (Currently amended), (Canceled), (Withdrawn), (Previously presented), (New), and (Not entered).

(1) *Claim listing.* All of the claims presented in a claim listing shall be presented in ascending numerical order. Consecutive claims having the same status of "canceled" or "not entered" may be aggregated into one statement (*e.g.*, Claims 1-5 (canceled)). The claim listing shall commence on a separate sheet of the amendment document and the sheet(s) that contain the text of any part of the claims shall not contain any other part of the amendment.

(2) *When claim text with markings is required.* All claims being currently amended in an amendment paper shall be presented in the claim listing, indicate a status of "currently amended," and be submitted with markings to indicate the changes that have been

made relative to the immediate prior version of the claims. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. Only claims having the status of "currently amended," or "withdrawn" if also being amended, shall include markings. If a withdrawn claim is currently amended, its status in the claim listing may be identified as "withdrawn-currently amended."

(3) *When claim text in clean version is required.* The text of all pending claims not being currently amended shall be presented in the claim listing in clean version, *i.e.*, without any markings in the presentation of text. The presentation of a clean version of any claim having the status of "original," "withdrawn" or "previously presented" will constitute an assertion that it has not been changed relative to the immediate prior version, except to omit markings that may have been present in the immediate prior version of the claims of the status of "withdrawn" or "previously presented." Any claim added by amendment must be indicated with the status of "new" and presented in clean version, *i.e.*, without any underlining.

(4) *When claim text shall not be presented; canceling a claim.*

(i) No claim text shall be presented for any claim in the claim listing with the status of "canceled" or "not entered."

(ii) Cancellation of a claim shall be effected by an instruction to cancel a particular claim number. Identifying the status of a claim in the claim listing as "canceled" will constitute an instruction to cancel the claim.

(5) *Reinstatement of previously canceled claim.* A claim which was previously canceled may be reinstated only by adding the claim as a "new" claim with a new claim number.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 4-17 and 20-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer et al (hereafter Schnurer) (U.S. Patent 5,842,002), in view of Nachenberg (U.S. Patent 6,357,008).

6. Schnurer and Nachenberg were cited in the last office action.

7. As to claim 1, Schnurer teaches the invention substantially as claimed including a computer-implemented method for executing an untrusted program [abstract, lines 1-2], comprising:

establishing a limited environment within a general environment [col. 6, lines 56-58; Figs. 3 and 4], wherein said limited environment comprises one or more mock resources [col. 4, lines 16-20, 22-26 and 47-49; col. 7, lines 3-8], wherein said general environment comprises one or more real resources [col. 4, lines 24-25; col. 7, lines 15-18], wherein programs executing within said limited environment cannot access the one or more real resources in said general environment [abstract; col. 5, lines 5-10; col. 7, lines 15-18];

executing at least a portion of an untrusted program within said limited environment [col. 7, lines 5-12]; and examining said limited environment after execution of at least said portion of said untrusted program to check for undesirable behavior exhibited by said untrusted program [col. 4, lines 32-36; col. 7, lines 12-15; 48, 50, 52, Fig. 1].

8. Schnurer does not specifically teach wherein said limited environment and said general environment are both provided by the same operating system. However, Schnurer disclosed trapping device within a network environment [col. 6, lines 56-58; Fig. 3 and 4]. In addition, Nachenberg teaches an antivirus program that includes a decryption, exploration and evaluation phases/modules causing a CPU emulator with virtual memory to simulate untrusted

programs/instructions [Nachenberg, col. l, lines 16-20; col. 5, lines 27-40; col.6, lines 52-58; col. 7, line 31-col. 8, line 47].

9. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have modified the teaching of Schnurer with the teaching of Nachenberg by implementing the limited environment in the same machine as the general environment if the limited environment is limited to protect a specific machine and to have an operating system within the machine providing both environments for the same reason to avoid the overhead of communicating through a network (i.e. an antivirus program running under an operating system protecting other programs/hardware/real resources running under the same operating system).

10. As to claim 4, Schnurer as modified teaches the invention substantially as claimed including wherein examining said limited environment comprises: determining whether a mock resource has been deleted [col. 4, lines 37-39; col. 7, lines 12-15; Nachenberg, col. 9, line 44]. Schnurer as modified does not specifically teach a particular mock resource. However, Schnurer disclosed if anything within the environment changes, is a sign of a virus [col. 7, lines 48-52], and Nachenberg disclosed signature scanning of known viruses [Nachenberg, col. 1, lines 22-45]. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that a deletion of a particular file such as a system file is an obvious sign of a virus (i.e. deletion of a particular system file that would cause instability to the operating system).

11. As to claims 5-7, these claims are rejected for the same reason as claim 4 above. In addition, Schnurer as modified teaches mock resource has been renamed or moved [Nachenberg, col. 9, lines 47-49], or altered [col. 7, line 48 to col. 8, line 26; Nachenberg, col. 9, lines 54-55].

12. As to claim 8, Schnurer as modified teaches the invention substantially as claimed including wherein said mock resource has a parameter associated therewith which changes when said mock resource is altered, and wherein determining whether said mock resource has been altered, comprises:

determining whether said parameter has changed [col. 7, line 48 to col. 8, line 26].

13. As to claim 9, Schnurer as modified does not specifically teach the step of determining whether said mock resource has been last updated. However, Schnurer disclosed that his system could detect any malicious act by the virus, including the activities of changing the FAT table and changing of the error checking algorithm [col. 7, lines 59-60; col. 8, lines 25-26; col. 4, lines 37-39]. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that common viral activities or critical behaviors exhibited by viruses would have included the updating of system resources as being considered and implemented in Schnurer's method of virus detection.

14. As to claim 10, this claim is rejected for the same reason as claim 4 above. In addition, Schnurer as modified teaches the invention substantially as claimed including wherein examining said mock environment comprises:

determining whether said mock resource has been accessed [col. 7, line 48 to col. 8, line 26].

15. As to claim 11, Schnurer as modified does not specifically teach wherein said mock resource contains one or more sets of content, and searching a particular portion of memory for at least one of said one or more sets of content. It is well known in the art that when a file gets accessed or altered, traces of the contents being accessed is located in the memory, in addition, Schnurer disclosed the determination of potential viral activities by examining "if anything within the environment changes..." [col. 7, line 48 to col. 8, line 26].

16. As to claim 12, Schnurer as modified teaches the invention substantially as claimed including providing information indicating behavior exhibited by said untrusted program [col. 7, line 25 to col. 8, line 26].

17. As to claims 13 and 14, Schnurer as modified teaches the invention substantially as claimed including wherein said information comprises indications of undesirable behavior exhibited by said untrusted program [col. 7, lines 48-52], and in response to a determination that

said untrusted program has exhibited undesirable behavior, taking corrective action [col. 8, lines 27-35; 52, Fig. 1].

18. As to claims 15 and 16, Schnurer as modified teaches the invention substantially as claimed including wherein taking corrective action comprises: deleting said untrusted program and warning to a user [col. 8, lines 27-35; 52, Fig. 1].

19. As to claims 17 and 20-32, these are computer readable medium comprising instructions claims that correspond to the method claims 1 and 4-16. Therefore, they are rejected for the same reason as claims 1 and 4-16 above.

20. Claims 3 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer and Nachenberg as applied to claims 1 and 17 above, in view of Basu et al (hereafter Basu) (U.S. Patent 6,836,888).

21. Basu was cited in the last office action.

22. As to claim 3, Schnurer and Nachenberg do not specifically teach wherein said limited environment comprise a shell in a UNIX operating system environment. However, Nachenberg disclosed different operating systems [Nachenberg, col. 6, lines 52-58]. In addition, Basu

teaches a shell program as a user interface to a sandbox in a UNIX operating system environment [Basu, col. 9, lines 17-22; col. 12, line 66-col. 13, line 5].

23. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have modified the teaching of Schnurer and Nachenberg with the teaching of Basu because the teaching of Basu can further increase the flexibility of Schnurer and Nachenberg's system by implementing the limited environment on different operating systems.

24. As to claim 19, this is a computer readable medium comprising instructions claims that correspond to the method claim 3. Therefore, it is rejected for the same reason as claim 3 above.

Response to Arguments

25. Applicant's arguments filed 12/4/06 have been fully considered but they are not persuasive.

26. In the remarks, Applicant argued in substance that:

a. The prior arts cited disclose emulation rather that actual execution, and that "executing at least a portion of an untrusted program within said limited environment" is not disclosed or suggested. The trapping device emulates the behavior of the virus code.

27. Examiner respectfully traversed Applicant's remarks:

28. As to point (a), Schnurer teaches simulating the host computer system [abstract], the emulation means provide an emulated environment fooling the virus into acting as if it were really present on the host system, catches the virus in the act of replicating, and attacking another program or destroying data [col. 7, lines 3-15]. As cited above, Schnurer clearly teaches that it is the host environment in which the virus executes that is emulated and not the virus code. More specifically, Schnurer teaches that data is written to the emulation box and checked whether simply data was written or whether executable code was written, force the executable to run and determine if a virus exist based on behaviors observed [col. 7, lines 29-52], therefore is very clear that the virus is indeed executed.

29. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Qing-Yuan Wu whose telephone number is (571) 272-3776. The examiner can normally be reached on 8:30am-6:00pm Monday-Thursday and alternate Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Thomson can be reached on (571) 272-3718. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Qing-Yuan Wu

Examiner

Art Unit 2194

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER